1-1-2010

Remote Access Forensics for VNC and RDP on Windows Platform

Paresh Kerai
Edith Cowan University

DOI: 10.4225/75/57b2a86540cde
8th Australian Digital Forensics Conference, Edith Cowan University, Perth Western Australia, November 30th 2010

Remote Access Forensics for VNC and RDP on Windows Platform

Paresh Kerai
School of Computer and Security Science
Edith Cowan University
Perth, Western Australia
pkerai@our.ecu.edu.au

Abstract

There has been a greater implementation of remote access technologies in recent years. Many organisations are adapting remote technologies such as Virtual Network Computing (VNC) and remote desktop (RDP) applications as customer support application. They use these applications to remotely configure computers and solve computer and network issues of the client on spot. Therefore, the system administrator or the desktop technician does not have to sit on the client computer physically to solve a computer issue.

This increase in adaptation of remote applications is of interest to forensic investigators; this is because illegal activities can be performed over the connection. The research will investigate whether remote protocols and applications do produce and leave valuable artefacts behind on Windows systems. The research aims to determine and retrieve any artefacts left behind remote protocols and applications in a forensic manner. Particular remote applications are selected to perform the research on and initial analysis will be performed on the applications to evaluate the potential forensic artefacts present on the computer system. The research will focus on Windows XP for analysis of the remote applications and find out what artefacts if any are left behind these systems.

Keywords

VNC, RBF protocol, man-in-middle attack, sniffing, 3DES, encryptions

INTRODUCTION

Mobile computing in organisations is becoming more common practise and is growing, which means the ability to remotely connect to networks is growing too (LaRose, 2010). To accomplish this, right recipe of equipment, protocols and applications are required.

The ability to access files, information and data from your work computer over the internet from home is very useful and productive for many organisations. Several remote access technologies are available to enable this kind of feature (Mike, 2007). Ideally, you can access the entire working environment over the wire from wherever you are currently sitting; this eliminates the need for synchronising files between the computers and laptops (Mike, 2007).

Current remote desktop software available does have a few downsides. Firstly that the current remote access technologies does not allow for lad-free control of a remote computer, and secondly that the computing experience will be certainly slower, than it would be if the person was seated next to the actual computer (Mike, 2007).

The increasing use of remote connectivity applications such as virtual networking communication (VNC), introduce threats to organisations and also to governments as illegal activities can be performed remotely on a system or network.

REMOTE ACCESS

Remote access is used to allow users to view and fully interact with information or data from one computer to another. Remote access simply uses a protocol over a TCP/IP connection. Many organisations and individuals use this protocol to monitor and troubleshoot remote computers and systems.

Remote access can be exploited by criminals and internet fraudsters to perform illegal activities and commit crime over the internet. The hackers and criminals can use this technology to perform crime from remote locations, making it harder to trace the crime as hackers are not using their computers to perform the acts,

instead they use a remote computer (Remote PC Access, 2009). Attackers can also place malware on the remote systems to steal the entire information pass through the network and sell it to competitors in money terms.

COMPUTER FORENSICS

Computer forensics is the process of obtaining, identifying, extracting, analysing, and documenting of computer evidence stored as data/digital/magnetically encoded information for use as evidence in civil, administrative and criminal cases. (Nelson et al., 2006); (Vacca, 2005). Forensic techniques are commonly used by many law enforcement organisations to bring criminals to justice. However, computer forensics need to be followed in a defined procedure; a handbook published by Standards Australia is currently used as a guide on how to carry and manage electronic evidence (HB171, 2003).

Computer Forensics Procedure

It is important to follow the procedure when performing an acquisition of the evidence in the crime scene and later following to perform the investigation in a forensically sound manner (Hannay, 2007). This is because the nature of the evidence shown to the court of law is intangible and volatile.

Basic methodology that is used to perform forensic investigation includes:

- Acquiring the evidence on the crime scene, without altering or damaging the evidence or causing minimal change to original evidence.
- Authenticating that the acquired evidence is the same as the original seized device or evidence; this can be done by chain of custody or document and obtaining photos as a proof.

Brown, (2006) has identified four major phases of a digital crime scene investigation these are collection, preservation, analysing and presentation.

VIRTUAL NETWORK COMPUTING (VNC)

Virtual network computing was first developed by the Olivetti and Oracle Research Laboratory (ORL) as their telephone system, allowing the organisation of the interface of X Windows application to be displayed on a remote machine (Morris, 2001). Since a large amount of bandwidth is required for the connection, a video tile that display devices such as Pen, LCD screen and ATM connection was developed by the organisation. In January 1999, AT & T labs bought and secured Olivetti and Oracle Research Laboratory (ORL), hence making VNC a project of AT & T labs, Cambridge UK (Morris, 2001).

This technology enabled computer users to access centralised and remote resources from widely available devices (Wannous & Nakano, 2010). Virtual network computing (VNC) is a thin client technology that can be used to display and work on a remote X window, which is a graphical user interface window of another computer (Waugh, 2002).

The application has two independent versions; the client and the server, both of which run on any platform. Therefore, this makes it perfect for those users who use the windows operating system to manage Unix operating systems and vice versa (Bezroukov, 2009). It also makes the application important for network and system administrators, as they would not have to attend each and every computer for troubleshooting; instead they use VNC to assign the task from one location (Bezroukov, 2009). There is also a VNC viewer written in Java, which can be accessed through a web browser.

VNC is currently going in many directions. When Olivetti and AT&T were slow to release the first VNC applications and this led to several independent VNC development projects. It is going to be very interesting to find out how VNC, as a project, will progress as original VNC developers are currently working with RealVNC (Waugh, 2002).

There are certain areas in which VNC efforts are lacking and under contention, Such areas include printing files and documents remotely and also fast and safe ways to transfer files from the viewer to the server (Waugh, 2002).

VNC Server

VNC server is initially configured to accept an incoming HTTP connection requested by the viewer over VNC default TCP ports (Wannous & Nakano, 2010). The VNC server and viewer negotiate the connection with mutually understanding encoding (Waugh, 2002). The server needs to be installed on the host system or machine and is currently available on Unix X window, Windows and Macintosh computer systems. The server needs to be defined, configured and installed on the host system or machine, to which the viewers have something to connect.

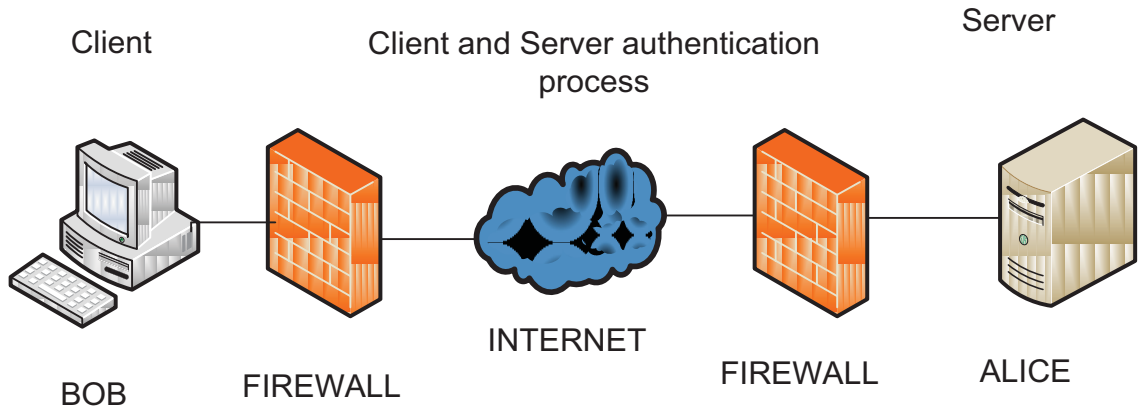
Communication over a VNC connection between the client and server is not completely encrypted, though the password used for the connection is encrypted by the DES or 3DES encryption standards depending on different VNC applications. This would be a concern for organisations as traffic could be intercepted and sniffed by an attacker over the network. However the PCAnywhere application has an add-on feature to version 1.0, for encrypting traffic between the connections (Green, 2004).

VNC Viewer

When the viewer is connected to the server, the user or administrator can connect to the remote server system and view the system. The viewer is currently available in many operating systems such as Unix X Window, Java, Windows, Macintosh 7.1 or higher and Windows CE 2.0 or later. The advantage of the viewer is that it does not require any installation and configuration like the server and can be run directly from a hard drive or any external electronic device. Interestingly the viewer can connect to the server and view any activity on the remote server without the server being controlled by the viewer. This can be used by administrators to monitor server activity remotely (Morris, 2001).

VNC Session Initiation

The following session initiation and authentication process that takes place between the viewer and the server.



- A Data Encryption Standard (DES) key (Luo, 2007) is used by both Bob and Alice endpoints for authentication.
- Bob connects to Alice and both exchange protocol version information.
- Alice generates a 16 byte key challenge and sends it to Bob.
- Bob then encrypts the received challenge with the DES key and sends it to Alice.
- Alice then encrypts the challenge key with DES and compares the hash with the key Bob send to her.
- If both keys match then access is granted to Bob, otherwise access is denied.

(Arce, 2001)

When the VNC connection is first established between the server and client, the former requests authentication from the client using a challenge response scheme, this usually prompts the client to input the session password. When the authentication process is completed, the server and client negotiate pixel format, desktop size and the encoding scheme to be used for the connection. Finally after the negotiation of the display settings, the session begins (AT&T Laboratories Cambridge, 1999).

MATERIALS

Various softwares and tools were used during the data collection, acquisition and conducting analysis on the images. The tools and software used for the research are summarised and explained below.

a) VMware application v 7.1.1 build-282343 – VMware is virtualisation software, this software will be used in the research as a base platform to install Windows XP operating systems for creating a scenario for the study. Then later the systems will be imaged for analysis and testing.
b) Windows XP operating system – Windows XP operating system will be used for the analyses and different service packs of Windows XP will be used for testing.
c) Forensic Tool Kit (Access Data) v 1.71 - Forensic Tool Kit by (Access Data) will be used in conjunction with other monitoring tools, to analyse the different computer systems that contains Windows XP operating system.
d) RealVNC v P4.5.4, UltraVNC v 1.0.8.2, TightVNC v 2.0.2 and TeamViewer v 5.0.8232 – these are different types of VNC application that are most commonly used by many individuals and organisations for remote access of computer systems. Therefore all these different applications will be used and tested on the machines.
e) Abel and Cain v 4.9.35 – This is a password recovery and sniffing tool developed for Windows operating systems. The application has various features to recover passwords, such as sniffing the internet traffic, recovering wireless network passwords, recording VOIP conversations and also cracking encrypted passwords using dictionary attacks, brute-force and cryptanalysis attacks (Cain & Abel, 2010). The tool will be used to recover and crack VNC passwords and to test the encryption of the protocols.
f) FTK Imager v 1.5.5.45 – FTK imager is a tool used to image physical and logical hard drive or any external devices as exact copy. The tool supports storage disks images in SMART's format, dd raw data format and also EnCase format. The tool will be used to image all the three Windows XP service packs. Since it uses supports dd format it is ideal for imaging.
g) Mount Image Pro v4.01 – this is a forensic tool that allows to mount raw images files also support other file formats, as logical drive on the computer. The tool will be used to mount the images on the testing computer to find encrypted passwords or recover remote session passwords.
h) Password Recovery Tools –Tools such as Elcomsoft 2009, VNC passview v 1.02 and Password Recovery bundle 2010 v 1.30 are going to be used for cracking the session initiation password of the VNC.
i) Sysinternals Suite – This is a troubleshooting utilities suite developed by Microsoft. The suite includes useful tools such as portmon, process explorer, TCPView, PsLogList, PsPasswd and many more (Russinovich, 2010); such tools will help the analysis of the images to look for artefacts of the remote protocols.
j) MiTeC Windows Registry Analyser 1.5.2.0 – this tool helps to view registry files of the acquired image for analysis of the registry system of the image.

The virtual machines and images will not be real evidence seized by law enforcement, but the systems will be configured in such a way that it can be used as real seized evidence.

ANALYSIS OF TEST DATA

The testing on the images is carried out using forensic tool kit (FTK) application and also mount image pro tool. FTK imager is used to acquire raw images of the Windows XP three service packs. The tool acquires raw dd image, this makes the images an exact copy of the system. After all the images are been tested using the procedure mentioned above in order to acquire test data for the images. Later the images are loaded on FTK tool kit and analysed on Windows XP test machine. Both set of images are analysed and all resulted in valuable test data.

ADSL router does not allow any type of remote connections between the computer network and outer networks (internet). This is because the router firewall does not have the remote protocols ports open. Therefore, for someone to use the remote connectivity features either VNC, they will have to allow the application ports to communicate with internet and outside networks. This can be done through the router firewall settings under port forwarding feature. The router firewall is configured to allow the remote protocols for communications.

Upon installing the VNC applications, they automatically configure the Windows firewall settings to allow the remote connections by opening the ports. However this is not the case in Windows XP service pack 1, the applications are not able to configure the firewall of XP service pack 1, and therefore connection is not possible

unless someone manually configures the firewall to open the ports. For the Windows XP service pack 2 and 3, firewall is automatically configured by VNC applications to open the ports.

TeamViewer is an application used for remote connection. It is different on how it works as compared to other VNC applications. This is because it neither uses the RFB protocol for connection nor 5900 and 5800 ports for connection and it uses HTTP port 80 for connection. It uses Advanced Encryption Standard (AES) for remote session password encryption with 128 byte string. This is very strong encryption standard as compared to DES and 3DES, used by other VNC applications.

In all Windows XP service packs, the firewall does not log any connection and network information of the computer by default. This is because firewall logging on Windows XP is not enabled; therefore no logs information can be obtained of any connections made using the VNC applications to other computers, unless firewall logging is enabled. VNC logging was enabled to retrieve the connection log information.

Also with VNC applications, the logging of the application is disabled by default, however for Team Viewer, upon installation it enables logging. Hence this will log the connections made to the application log file.

Event viewer is a component of Windows operating system and lets the users and administrators view the event logs on the local computer. The event log service records the application, security and system events in Windows XP under event viewer. This is a critical place for administrators and forensics investigators to check for application, security and system logs for investigation purposes and also to identify and analyse the source of current system problems (Microsoft Support, 2007). Real VNC and Ultra VNC logs the connection details in the application log under event viewer on the destination computer, and not on the host or local computer. Therefore if a remote connection is initiated using Real VNC and Ultra VNC the log information of the connection is found on the destination computer, and not on the local computer. Tight VNC, Team Viewer do not log any information under event viewer.

All the VNC applications store the application and connection settings under the Windows registry. Windows registry is the core configurations database for Windows NT/ Windows 2000/ XP/ server 2003/ server 2008/ Vista and Windows 7. It stores information about the tuning parameters, device configuration, application configurations and user settings and preferences (Russinovich, 2000). The registry is divided into five different set of discrete files called *hives.* "A registry hive is a group of keys, sub keys and values in that has set of supporting files that contain backup of its data" (Microsoft support, 2008). The table below explains what each of the hives contains:

Windows PC	Settings stored
HKEY_LOCAL_MACHINE (HKLM)	Stores information about local computer, such as system memory, devices, drivers, and hardware settings.
HKEY_CLASSES_ROOT (HKCR)	Stores information used by various OLE technologies, file association and COM object registration.
HKEY_CURRENT_USER (HKCU)	Stores information about the current user logged on.
HKEY_USERS (HKU)	Stores information about all the accounts on the local computer.
HKEY_CURRENT_CONFIG (HKCC)	Stores information about the current hardware profile used by the local computer.

Table 1 *Windows Registry system Hives*

(Microsoft support, 2008)

VNC applications store the settings under three hives, **HKEY_LOCAL_MACHINE (HKLM), HKEY_CURRENT_USER (HKCU)** and **HKEY_USERS (HKU).** The applications store information such as client IP addresses the local computer connected to, encrypted remote session passwords, desktop screen settings, graphic settings, printer settings and connection settings. The IP address stored is private IP address of the client. Server remote session password stored on the registry is vulnerable and easy to crack. During the experimentation phase the author found out that it is easy to crack the session passwords using Abel and Cain software. The software contains a feature to decrypt VNC password for up to 8 characters long.

All VNC applications and Team Viewer support file transfer feature.

Windows Registry Analysis

This shows the test results of the registry system analysis of the acquired images and shows what types of artefacts were found during the experimental phase of the research. Two applications namely: Alien registry viewer and MiTeC windows registry analyser were used side by side for the analysis of the registry files. All the registry keys were extracted and exported on a computer for analysis. The hash values were created of the files for integrity purposes. The hashes of the files are located in the Appendix A. Figures in appendix C show some registry hives snagged for reference on how and where the applications store the settings under the Windows registry.

Image 1 (Windows XP service pack 1).

The table below summarises the artefacts left behind by the VNC applications under the registry system of Windows XP service pack 1

VNC applications	Artefacts left under registry system
Ultra VNC	- Under HKEY_CURRENT_USER\Software\ORL\VNCviewer\MRU, the application stores client private IP addresses the computer connected. - Under HKEY_CURRENT_USER\Software\ORL\VNCviewer\History, the application stores the connection settings for each client IP addresses.
Real VNC	- Under HKEY_LOCAL_MACHINE\software\RealVNC\WinVNC4 , the application stores the RSA private key generated by the VNC server during the connection. - Under HKEY_CURRENT_USER \Software\RealVNC\VNCViewer4\MRU, the application stores the history of the client private IP addresses the computer made connections to. - Under HKEY_LOCAL_MACHINE\software\RealVNC\WinVNC4, the application stores the local computer VNC server session password which is encrypted. It also stores It also stores View only password and Admin password also encrypted under this value. - Under HKEY_LOCAL_MACHINE\Software\RealVNC\VNC Address Book, it stores the connection settings and connection password of a connection that the user saved for future quick connection.
Tight VNC	- Under HKEY_LOCAL_MACHINE\Software\TightVNC\Server, application stores the VNC server session password of the local computer, which is typically encrypted. The application also stores the connection settings defined by the user. - Under HKEY_CURRENT_USER \Software\TightVNC\Server, application also stores the VNC server session password of the local computer, which is typically encrypted. The application also stores the connection settings defined by the user.
Team Viewer	- Under HKEY_CURRENT_USER \Software\TeamViewer\Version5, the application stores the history of the client IDs, the local computer connected to. - Under HKEY_LOCAL_MACHINE\Software\ TeamViewer\Version5, the application stores the private and public keys of the remote connection and also other settings relating to the connection.

Table 2 *VNC applications settings stored under the registry system*

Image 2 (Windows XP service pack 2)
The table below summarises the artefacts left behind by the VNC applications under the registry system of Windows XP service pack 2.

VNC applications	Artefacts left under registry system
Ultra VNC	- Under HKEY_CURRENT_USER\Software\ORL\VNCviewer\History, the application stores client private IP addresses the computer connected. - Under HKEY_CURRENT_USER\Software\ORL\VNCviewer\History, the application stores the connection settings for each client IP addresses. - Under HKEY_CURRENT_USER\Software\ORL\WinVNC, the application stores the computer's VNC server password which is typically encrypted.
Real VNC	- Under HKEY_LOCAL_MACHINE\software\RealVNC\WinVNC4 , the application stores the RSA private key generated by the VNC server during the connection. - Under HKEY_CURRENT_USER \Software\RealVNC\VNCViewer4\MRU, the application stores the history of the client private IP addresses the computer made connections to. - Under HKEY_LOCAL_MACHINE\Software\RealVNC\WinVNC4, the application stores the local computer VNC server session password which is encrypted. It also stores View only password and Admin password also encrypted under this value. - Under HKEY_LOCAL_MACHINE\Software\RealVNC\VNC Address Book, it stores the connection settings and connection password of a connection that the user saved for future quick connection.
Tight VNC	- Under HKEY_LOCAL_MACHINE\Software\TightVNC\Server, the Tight VNC application stores the VNC server session password of the local computer, which is typically encrypted. The application also stores the connection settings defined by the user. - Under HKEY_CURRENT_USER \Software\TightVNC\Server, application stores the VNC server session password of the local computer, which is typically encrypted. The application also stores the connection settings defined by the user.
Team Viewer	- Under HKEY_CURRENT_USER \Software\TeamViewer\Version5, the application stores the history of the client IDs, the local computer connected to. - Under HKEY_LOCAL_MACHINE\Software\ TeamViewer\Version5, the application stores the private and public keys of the remote connection and also other settings relating to the connection.

Table 3 *VNC applications, TeamViewer settings stored under the registry system*

Image 3 (Windows XP service pack 3)
The table below summarises the artefacts left behind by the VNC applications under the registry system of Windows XP service pack 3.

VNC applications	Artefacts left under registry system
Ultra VNC	- Under HKEY_CURRENT_USER\Software\ORL\VNCviewer\History, the application stores client private IP addresses the computer connected. - Under HKEY_CURRENT_USER\Software\ORL\WinVNC, the application stores the computer's VNC server password which is typically encrypted. - Under HKEY_CURRENT_USER\Software\ORL\VNCviewer\History, the

	application stores the connection settings for each client IP addresses.
Real VNC	- Under HKEY_LOCAL_MACHINE\software\RealVNC\WinVNC4 , the application stores the RSA private key generated by the VNC server during the connection. - Under HKEY_CURRENT_USER \Software\RealVNC\VNCViewer4\MRU, the application stores the history of the client private IP addresses the computer made connections to. - Under HKEY_LOCAL_MACHINE\Software\RealVNC\WinVNC4, the application stores the local computer VNC server session password which is encrypted. It also stores View only password and Admin password also encrypted under this value. - Under HKEY_LOCAL_MACHINE\Software\RealVNC\VNC Address Book, it stores the connection settings and connection password of a connection that the user saved for future quick connection.
Tight VNC	- Under HKEY_LOCAL_MACHINE\Software\TightVNC\Server, the Tight VNC application stores the VNC server session password of the local computer, which is typically encrypted. - Under HKEY_CURRENT_USER \Software\TightVNC\Server, application stores the VNC server session password of the local computer, which is typically encrypted. The application also stores the connection settings defined by the user.
Team Viewer	- Under HKEY_CURRENT_USER \Software\TeamViewer\Version5, the application stores the history of the client IDs, the local computer connected to. - Under HKEY_LOCAL_MACHINE\Software\ TeamViewer\Version5, the application stores the private and public keys of the remote connection and also other settings relating to the connection. - Under HKEY_LOCAL_MACHINE\Software\ TeamViewer\Version5, the application also stores the security password used for connection, typically encrypted with AES encryption standard.

Table 4 *VNC applications, TeamViewer settings stored under the registry system*

LOG FILE ANALYSIS

Log files carry important and an enormous amount of information regarding the remote connection. Log files are useful because of the information it consists of such as date and time of logs and who the computer is connected to and which computer disconnected or closed the connection. Figures in appendix D (pg 124 – 137) show some log files extracted from the images that contain important information on whether the computer had any remote connections. Event log explorer was used to view the log information of the image. All the event log files were extracted and exported to a computer for analysis. The hash values were created of the files for integrity purposes. The hashes of the files are located in the Appendix B (pg 71-74).

Image 1 (Windows XP service pack 1)

The table below summarises the artefacts left behind by VNC as log information on the Windows file system for Windows XP service pack 1.

VNC applications	Artefacts left under file system
Ultra VNC	- Ultra VNC leaves log information under the application event viewer of receiving computer's IP address and not of the host computer. - Under C:\Program Files\UltraVNC, the application leaves a WInVNC log file that consists of debug information.

Real VNC	- Real VNC leaves log information under the application event viewer of receiving computer's IP address and not of the host computer. - Real VNC stores saved connections under the C:\Documents and Settings\Administrator\Application Data\RealVNC. The saved connection contains the connection settings including the password for the connection.
Tight VNC	- Tight VNC places a log file under C:\Documents and Settings\Administrator\Application Data\TightVNC. The folder contains a log file of the application, however the file is empty and no log information is displayed, despite the connections.
Team Viewer	- Team Viewer typically stores log information under C:\Documents and Settings\Administrator\Application Data\TeamViewer folder. The folder contains two files. Firstly connections file and TeamViewer5_log file, both files contain connection information including file transfer logs.
Firewall	- Firewall log is placed under the C:\WINDOWS\pfirewall.log. The log information contains the all incoming and outgoing network information of the local network.

Table 5 *Image 1 log information summary*

Image 2 (Windows XP service pack 2)

The table below summarises the artefacts left behind by VNC as log information on the Windows file system for Windows XP service pack 2.

VNC applications	Artefacts left under file system
Ultra VNC	- Ultra VNC leaves log information under the application event viewer of receiving computer's IP address and not of the host computer. - Ultra VNC places a log file under C:\Program Files\UltraVNC named mslogon. However there was no log file located in Image 1, therefore the application does not have any log file in Windows XP service pack. The file consists of client IP address and date and time the connection was received and ended. - Under C:\Program Files\UltraVNC, the application leaves a WInVNC log file that consists of debug information.
Real VNC	- Real VNC leaves log information under the application event viewer of receiving computer's IP address and not of the host computer. - Real VNC stores saved connections under the C:\Documents and Settings\Administrator\Application Data\RealVNC. The saved connection contains the connection settings including the password for the connection.
Tight VNC	- Tight VNC places a log file under C:\Documents and Settings\Administrator\Application Data\TightVNC. The folder contains a log file of the application, however the file is empty and no log information is displayed, despite the connections.
Team Viewer	- Team Viewer typically stores log information under C:\Documents and Settings\Administrator\Application Data\TeamViewer folder. The folder contains two files. Firstly connections file and TeamViewer5_log file, both files contain connection information including file transfer logs.
Firewall	- Firewall log is placed under the C:\WINDOWS\pfirewall.log. The log information contains the all incoming and outgoing network information of the local network.

Table 6 *Image 2 log information summary*

Image 3 (Windows XP service pack 3)

The table below summarises the artefacts left behind by VNC as log information on the Windows file system for Windows XP service pack 3.

VNC applications	Artefacts left under file system
Ultra VNC	- Ultra VNC leaves log information under the application event viewer of receiving computer's IP address and not of the host computer.

	- Ultra VNC places a log file under C:\Program Files\UltraVNC named mslogon. However there was no log file located in Image 1, therefore the application does not have any log file in Windows XP service pack. The file consists of client IP address and date and time the connection was received and ended. - Under C:\Program Files\UltraVNC, the application leaves a WInVNC log file that consists of debug information.
Real VNC	- Real VNC leaves log information under the application event viewer of receiving computer's IP address and not of the host computer. - Real VNC stores saved connections under the C:\Documents and Settings\Administrator\Application Data\RealVNC. The saved connection contains the connection settings including the password for the connection.
Tight VNC	- Tight VNC places a log file under C:\Documents and Settings\Administrator\Application Data\TightVNC. The folder contains a log file of the application, however the file is empty and no log information is displayed, despite the connections.
Team Viewer	- Team Viewer typically stores log information under C:\Documents and Settings\Administrator\Application Data\TeamViewer folder. The folder contains two files. Firstly connections file and TeamViewer5_log file, both files contain connection information including file transfer logs.
Firewall	- Firewall log is placed under the C:\WINDOWS\pfirewall.log. The log information contains the all incoming and outgoing network information of the local network.

***Table** 7 Image 3 log information summary*

CONCLUSION

Remote access protocols and applications provide a unique graphical user interface access to users to remote computers. Therefore the users can connect to a remote computer using remote desktop applications and perform tasks and functions as if they are sited next to the computer. Remote access simply uses a protocol over a TCP/IP connection. Many organisations and individuals use this protocol to monitor and troubleshoot remote computers and systems.

Remote access can be exploited by criminals and internet fraudsters to perform illegal activities and commit crime over the internet. Therefore this has significant potential to law enforcement agencies, government and other investigative agencies, as analysis on the applications may provide a way to track down the suspected cyber criminals.

As the adaption of the remote technologies is increasing, as such the investigators are also gathering forensic methods to recover potential artefacts left behind by theses remote technologies.

Future research in this area needs to be done to find out the degree of information and artefacts left behind by remote access protocols. The reason why further research is needed is that still a large amount of information can be retrieved from different remote applications and on different operating system platforms. Further analysis could potentially provide necessary or important information that is of forensic interest to investigators.

The research conducted and explained in this thesis has demonstrated that it is possible to retrieve any artefacts produced and left behind by the remote access protocols and applications in forensic sound manner. Information such as IP addresses and the server name it connected to, is still important information as the other party can be identified by their private IP address that was used to connect to the computer.

The analysis explained in this thesis will help forensic analysts and investigators to fight cyber crime over the internet.

REFERENCES

Arce, I. (2001). Weak authentication in ATT VNC allows man-in-the-middle attack. Retrieved 6 May 2010, from http://www.securiteam.com/securitynews/5ZP0P1535W.html

AT&T Laboratories Cambridge. (1999). VNC - How it works. Retrieved 4th May 2010, 2010, from http://virtuallab.tu-freiberg.de/p2p/p2p/vnc/ug/howitworks.html

Bezroukov, D. N. (2009). VNC -- The Essential Sysadmin Tool. Retrieved 5th August 2010, from http://www.softpanorama.org/Xwindows/vnc.shtml

Cain, & Abel. (2010). Cain & Abel. Retrieved 12th June 2010, from http://www.oxid.it/cain.htm

Green, R. (2004). Using Virtual Network Computing (VNC) to remotely access ODB. Retrieved 4th August 2010, from organizersdb.org/0.9/odbremote.pdf

Hannay, P. (2007). Acquisition of historical location data in a forensically sound and non-invasive manner for the TomTom One Satellite Navigation Unit. Edith Cowan University, Perth.

HB171. (2003). HB171: Guidelines for the management of IT evidence : handbook. Sydney: Standards Australia.

Kruse, W. G., & Heiser, J. G. (2002). Computer Forensics: Incident Response Essentials. Boston, MA: Addison-Wesley.

LaRose, M. (2010). What Are Remote Access Technologies? Retrieved 4th August 2010, 2010, from http://www.ehow.com/about_5046061_remote-access-technologies.html

Luo, V. C. (2007). Tracing USB Device artefacts on Windows XP operating system for forensic purpose. Paper presented at the Australian Digital Forensics Conference, Perth.

Microsoft Support. (2007). How to view and manage event logs in Event Viewer in Windows XP. Retrieved 13th September 2010, 2010, from http://support.microsoft.com/kb/308427

Microsoft support. (2008). Windows registry information for advanced users. Retrieved 5th May 2010, 2010, from http://support.microsoft.com/kb/256986

Mike. (2007). Beginners Guide: Remote Access to Computers. Retrieved 3rd August 2010, 2010, from http://www.pcstats.com/articleview.cfm?articleID=1441

Morris, P. (2001). Understanding Virtual Network Computing. PC Network Advisor(130), 9-13.

Remote PC Access. (2009). The Authorities Have A Tough Time With Remote Access. Retrieved 21st August 2010, from http://www.remotepcaccess.org/authorities-remote-access.html

Russinovich, M. (2000). Inside the Registry *Windows NT magazine* Retrieved 10th September 2010, 2010, from http://technet.microsoft.com/en-us/library/cc750583.aspx

Russinovich, M. (2010). Sysinternals Suite. Retrieved 14th May 2010, 2010, from http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx

Vacca, J. R. (2005). Computer forensics. Hingham, Mass: Charles River Media.

Wannous, M., & Nakano, H. (2010). NVLab, a Networking Virtual Web-Based Laboratory that Implements Virtualization and Virtual Network Computing Technologies. IEEE TRANSACTIONS ON LEARNING TECHNOLOGIES, 3.

Waugh, T. (2002). VNC Where it came from, where it's going. Retrieved 3/08/2010, from http://cyberelk.net/tim/articles/VNC/